UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of:

Various devices, more fully described in Attachment A, currently at the U.S. Department of Homeland Security, 790 North Milwaukee Street, Milwaukee, WI.

Case No. 19-896M(NJ)

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed:

See Attachment B

The basis for the search under Fed. R. Crim P. 41(c) is:

- ☒ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☐ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to violations of: Title 18, United States Code, Sections 1591 and 2423(c).

The application is based on these facts: See attached affidavit.

☐ Delayed notice of _____ days (give exact ending date if more than 30 days:_____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Kevin C. Wrona, HSI
Printed Name and Title

Sworn to before me and signed in my presence:

Date: August 13, 2019

Judge's signature

City and State: Milwaukee, Wisconsin

Hon. Nancy Joseph, U.S. Magistrate Judge
Printed Name and Title

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Kevin C. Wrona, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information as described in Attachment B.

2. I am a Special Agent with the U.S. Department of Homeland Security, U.S. Immigration and Customs Enforcement, Homeland Security Investigations ("HSI"), and have been so employed since June 2010. I am currently assigned to the HSI Office of the Resident Agent in Charge in Milwaukee, Wisconsin. My duties include investigating criminal violations relating to child sexual exploitation and child pornography. I have received training in the investigation of child pornography and child sexual exploitation offenses.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property (here after known as "Devices") to be searched for violations of Title 18, United States Code, Sections 1591 and 2423(c) are:

a. Lenovo laptop computer, Serial Number: YB10215587;
b. Black Samsung Cellphone, Serial Number: RF1F6151AVM;
c. SanDisk Ultra 32GB Micro SD card, Serial Number: 4226CM32M19y;
d. DT101 G2 8GB thumb drive; and
e. Apacer thumb drive

The Devices are currently at the U.S. Department of Homeland Security Office located at 790 N. Milwaukee Street, Milwaukee, Wisconsin, in evidence.

5. The applied-for warrant would authorize the forensic examination of the Devices for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. On June 20, 2018, I received CyberTip (CT) 35013606 from NCMEC regarding multiple Facebook usernames that appeared to be engaged in sexually explicit communications with minors. The CT was reported to NCMEC directly from Facebook, and included Facebook usernames, Facebook user ID numbers, e-mail addresses and internet protocol (IP) addresses used to access the Facebook accounts. The account of Don Stevenson and Donald White were reported in the CT. The Don Stevenson account was assigned the Facebook user ID 100012891004557, with a registered e-mail address of RUNDONRUN@YAHOO.COM and the use of IP addresses: 124.120.235.50, 219.74.114.109, and 49.145.131.152, which geolocate to Bangkok, Thailand; Singapore; and Cebu City, Philippines, respectively. The Donald White account was assigned the Facebook user ID 100025143570455, with a registered e-mail address of DONWHITECEBU@GMAIL.COM and the use of IP addresses: 172.220.77.181, 2605:a000:bce0:2c00:b17b:8b26:1673:cfbf, and 2605:a000:bcc0:b100:ad38:bd92:2cc3:fd86, which geolocate to Madison, Wisconsin; New Berlin, Wisconsin, and West Allis, Wisconsin, respectively. The CT also provided Facebook account information for the three (3) alleged minor females the Don Stevenson and Donald White accounts were in contact with, to include IP addresses. The CT indicated that the three IP addresses used by the alleged minor females were: 175.158.226.178, 49.151.80.69, and 180.190.171.56, all three of which geolocated to the Philippines.

7. The following Facebook messenger chats[1] were also provided in the CT:

a. Chats between the Don Stevenson account and an unidentified female A.L. account on September 22, 2017:

[Don Stevenson (100012891004557) - 09/22/2017 2:46:37am PDT]
If ur here, I give you a big hug.

[A.L. (100014305757229) - 09/22/2017 2:46:55am PDT]
heheehe

[Don Stevenson (100012891004557) - 09/22/2017 2:47:21am PDT]
and your first kiss.. ha ha ha.. joking again.

[A.L. (100014305757229) - 09/22/2017 2:47:33am PDT]
hmmmmn

[Don Stevenson (100012891004557) - 09/22/2017 2:48:36am PDT]
on your cheek

[Don Stevenson (100012891004557) - 09/22/2017 2:50:13am PDT]
And boobs..

b. Chats between the Donald White account and a Minor Victim 1 (here after referred to as MV1) account on May 14, 2018:

Donald White (100025143570455) - 2018/05/14 8:12am PDT
We can take shower?

MV1 (100023948806018) - 2018/05/14 8:13am PDT
yes

Donald White (100025143570455) - 2018/05/14 8:16am PDT
Thank you in advance

MV1 (100023948806018) - 2018/05/14 8:16am PDT
ok

---

[1] Facebook Messenger is a chat application in which which allows individual or a group of Facebook users to engage in online chats. Facebook and Facebook Messenger are both applications which can be accessed on both a computer, as well as a mobile device, such as a cellphone or tablet.

Donald White (100025143570455) - 2018/05/14 8:16am PDT
We can be lovers?

MV1 (100023948806018) - 2018/05/14 8:16am PDT
ok

c. Chats between the Donald White account and MV1 on May 21-22, 2018:

MV1 (100023948806018) - 2018/05/21 11:06pm PDT
How old ar you

Donald White (100025143570455) - 2018/05/21 11:07pm PDT
50 ... and you?

Donald White (100025143570455) - 2018/05/21 11:10pm PDT
How old are you?

MV1 (100023948806018) - 2018/05/21 11:56pm PDT
13

Donald White (100025143570455) - 2018/05/22 12:10am PDT
Oh. So young. I will be kind and respectful

d. Chats between the Donald White account and an unidentified female S.E. account on April 17, 2018:

Donald White (100025143570455) - 2018/04/17 10:51pm PDT
My friend asks if you are a virgin

S.E. (100014674219418) - 2018/04/17 10:52pm PDT
Yes I'm virgin

Donald White (100025143570455) - 2018/04/17 10:52pm PDT
We respect that

S.E. (100014674219418) - 2018/04/17 10:52pm PDT
Hah

Donald White (100025143570455) - 2018/04/17 10:53pm PDT
But we can cure that if you wish

[...]

S.E. (100025143570455) - 2018/04/17 11:00pm PDT

Can you show boobs on video call?

Additionally in the CT, the Don Stevenson and Donald White accounts were linked by machine cookies to a third a account which used the username Don Stenson. Facebook provided the associated account via "cookie" technology. "Cookies" are a small text file created by a website that is stored in the user's computer either temporarily or permanently on the hard disk. "Cookies" provide a way for the website to recognize you and keep track of your preferences. This information indicated all three Facebook accounts were being logged into using the same electronic device.

8. An HSI liaison to NCMEC conducted research into the various combinations of the first and last names and dates of birth for the White/Stevenson/Stenson Facebook accounts. The HSI liason identified an individual named: Donald Arthur STENSON, DOB: XX/XX/1956, with an associated address of: 2939 S. 101st St., Milwaukee, WI 53227.

9. As noted above, the CT provided the IP addresses used by the White/Stevenson/Stenson accounts to log into Facebook. On September 14, 2018, a DHS summons was sent to Charter Communications, requesting subscriber information on IP addresses: 172.220.77.181, 2605:a000:bce0:2c00:b17b:8b26:1673:cfbf, and 2605:a000:bcc0:b100:ad38:bd92:2cc3:fd86, which were IP addresses associated with the Donald White account. On September 14, 2018, Charter responded to the summons indicating that IP addresses: 2605:a000:bce0:2c00:b17b:8b26:1673:cfbf and 2605:a000:bcc0:b100:ad38:bd92:2cc3:fd86 were registered to John Burgdorff, XXXXXXX, West Allis, WI 53227, XXXXX@wi.rr.com,XXX-XXX-1463 and XXX-XXX-9792. It also indicated that IP address: 172.220.77.181 is registered to: Ellen Jessen, XXXXXX., Madison, WI 53714, XXX-XXX-7046, and

XXXXXX@charter.net. There were no DHS summonses served on the IP addresses associated with the Don Stevenson account, as those addresses were based in foreign countries.

10. As the investigation continued, HSI conducted a search into STENSON's travel history. HSI confirmed that STENSON traveled to the Philippines on multiple occasions since 2007, most recently between on or about January 6, 2019 and on or about January 22, 2019. Since November of 2015, Philippine travel records indicate that STENSON would arrive from Bangkok, into either Manila or Cebu, later departing Manila or Cebu to Bangkok. In addition to locating travel records, the HSI Attaché in Manila worked with Philippine authorities to identify and confirm the ages of the three possible minor female victims cited in the CT.

11. On March 21, 2019, HSI the Attaché in Manila contacted HSI Milwaukee. Between March 18, 2019 and March 21, 2019, HSI Manila, with the assistance of the HSI Manila Transnational Criminal Investigative Unit (TCIU), located and identified four (4) victims who are Philippine nationals that described sexual acts and conversations that took place between themselves and STENSON. One of the victims is now an adult, but was sexually abused as a minor, and the other three (3) victims are 13, 15, and 16 years of age. The four victims positively identified STENSON as the person who molested them by encircling the picture of STENSON through a photographic line-up.

12. During an interview by Philippine authorities, one of the four minor females stated that she met STENSON in 2017, when she was 12 years old. She stated that in October 2017, she and other underage minor victims met STENSON at his hotel room at the Hotel Le Carmen in Cebu and proceeded to masturbate him while STENSON fondled their breasts. She stated that after they finished, STENSON paid each of the minors money. She stated that she would masturbate STENSON once a week over the course of three weeks. She further stated that in addition to

money, STENSON gave her gifts, including food, clothing, a laptop, a cellphone and a tablet. Additionally, she stated that STENSON used a Facebook account with the username "Don Chonmanee."

13. On May 8, 2019, federal search warrants for the following Facebook accounts: Don Stevenson (FB ID#: 100012891004557), Donald White (FB ID#: 100025143570455), Don Stenson (FB ID: 1529468944), and Don Chonmanee (FB ID: 100009337719641) were issued by U.S. District Court for the Eastern District of Wisconsin and served on Facebook on May 8, 2019.

14. On May 17, 2019, Facebook responded to the search warrants on the accounts for: Don Stevenson (FB ID#: 100012891004557), Donald White (FB ID#: 100025143570455), Don Stenson (FB ID: 1529468944), and Don Chonmanee (FB ID: 100009337719641). The search warrant returns showed the IP addresses used to log into the accounts, as well as message logs and transcripts between those accounts and other Facebook users on Facebook Messenger. Further, the search warrant returns contained the pictures and messages for each account. Each account contained pictures shared by the account user of an individual who appears to be STENSON. Based on my training and experience, the machine cookies for each Facebook account, and my review of the search warrant return data for each Facebook account, it appears the Facebook user for the Stevenson/White/Chonmanee/Stenson accounts are same user based on the photos that look like the same person, that being STENSON, and the conversations contained in each account whereby the user is chatting with what appear to be minors in a sexual manner. Further, the Facebook users, using each Facebook account, indicated they planned to travel to the Philippines and expressed an interest in engaging in sexual activity with minor females.

15. After reviewing the full Facebook search warrant returns for each account, the following is a small example of some of the Facebook messenger chats relevant to this investigation:

a. Chats between the Stevenson account and A.L. are as follows:

-9/22/2017 - 09:42:52 UTC – Stevenson: ahahaha.. my excitement might include an erection.. ha ha ha.. sorry joke.
-9/22/2017 – 09:46:37 UTC – Stevenson: If ur here, I give you a big hug.
-9/22/2017 – 09:46:55 UTC – A.L.: heheehe
-9/22/2017 – 09:47:21 UTC – Stevenson: and your first kiss.. ha ha ha.. joking again.
-9/22/2017 – 09:48:36 UTC – Stevenson: on your cheek
-9/22/2017 – 09:50:13 UTC – Stevenson: And boobs…
-9/23/2017 – 11:35:44 UTC – Stevenson sends a picture that appears to be STENSON, holding up two (2) Hershey chocolate bars and one (1) Kit-Kat bar
-9/25/2017 – 12:44:45 UTC – Stevenson: And you want me to keep the camera on when I take a shower? ha ha ha
9/25/2017 – 12:47:25 UTC: Stevenson: Do you want to see my penis or banana before you close the call?

b. Chats between the Stevenson account and Minor 1, which is the account of an identified minor, are as follows:

-07/02/2017 – 11:14:52 UTC – Stevenson: Ohh..yes. U need the cp. I understand. And after bonding, it is possible.
NOTE: in this context, "cp" stands for cell phone
[…]
-07/02/2017 – 11:17:31 UTC – Stevenson: Do you study school, my dear?
-07/02/2017 – 11:17:50 UTC – Minor 1: Yes why my daer
-07/02/2017 – 11:18:27 UTC – Stevenson: Grade 7?
-07/02/2017 – 11:19:24 UTC – Minor 1: No grade 8na ako my deat
-07/12/2017 – 06:53:34 UTC – Stevenson: we will meet and bond next month
-07/12/2017 – 06:57:18 UTC – Minor 1: yes I waht your bonding next month

c. Chats between the Stevenson account and Minor 2, which is the account of another identified minor, are as follows:

-07/10/2017 – 23:54:27 UTC – Minor 2: Don u give cellphone
-07/10/2017 – 23:54:38 UTC – Minor 2: Pleass
-07/10/2017 – 23:55:17 UTC – Stevenson: yesss….. after bonding.. okay..
-07/10/2017 – 23:55:48 UTC – Minor 2: What bonding
-07/10/2017 – 23:56:13 UTC – Stevenson: I don't know.. ha ha..

[…]
-07/10/2017 – 23:56:31 UTC – Stevenson: bf/gf bonding? Ha ha ha

d. Chats between the Stevenson account and Minor 3, which is the account of another identified minor are as follows:

-11/25/2017 – 06:01:42 – Minor 3 sends Stevenson a picture of three young females who appear to be in the back of a vehicle. The female closest to the camera is wearing a black t-shirt with white lettering and a cartoon monster on it.

NOTE the identities of the three females have not been established

-11/25/2017 – 06:01:53 UTC – Minor 3: On going now

-11/25/2017 – 06:03:20 UTC – Stevenson: Ok. Don't get wet.

-11/25/2017 – 07:57:19 UTC – Minor 3 sends Stevenson nine (9) photographs. The images are of the female in the black t-shirt with white lettering and a cartoon monster and who appears to be with STENSON, in a room that appears to have similar features to a room at Hotel Le Carmen, which is the same hotel room the victims identified as the one where they would meet STENSON.

e. Chats between the Stevenson account and Minor 4, which is the account of another identified minor, are as follows:

-03/20/2018 – 13:10:39 UTC – Stevenson: Matt does not know when he will go to Cebu

-03/20/2018 – 13:12:11 UTC – Minor 4: Oh my god im excited to see matt

-03/20/2018 – 13:14:30 UTC – Stevenson: I will tell him he should go there.. He really likes to make love to pregnant girls

NOTE: as explained below, Minor 4 was forensically interviewed and stated that her birthday is June 4, 2001 and she was 17 years old and was four (4) months pregnant when she had sexual intercourse with STENSON

f. Chats between the Stevenson account and "Jon Bedford" are as follows:

-09/04/2017 – 14:12:01 UTC – Stevenson: Weird because any gal in my stable that I told to take off for any days other than maybe exams, they'd do it.

-09/05/2017 – 10:51:55 UTC – Stevenson sends Bedford a picture that appears to be STENSON laying in bed with two younger looking females, with one of them smiling at the camera

-09/05/2017 – 10:52:12 UTC – Bedford: Wow

-09/05/2017 – 10:52:29 UTC – Stevenson: Gotta get a last minute massage..

-09/05/2017 – 10:53:09 UTC – Bedford: Ok. Say hi to smiling girls

-09/05/2017 – 10:53:17 UTC – Stevenson: [Minor 4] and [Minor 3]

g. Chat between the Stevenson account and Vhasin Akohw Touh are as follows:

-08/20/2017 – 09:22:52 UTC – Stevenson: text me.. 09398220050
-09/17/2017 – 08:34:23 UTC – Stevenson: I know.. u will chupa or anal sex.. But NO tongue kiss.. No french kiss!!
-09/17/2017 – 08:34:48 UTC – Vhasin: Hahahahahahah noooo
-11/04/2017 – 09:15:20 UTC – Vhasin: And you have another ring for me?
-11/04/2017 – 09:16:48 UTC – Stevenson: not until after your debut[2].. An engagement ring
-11/04/2017 – 10:59:59 UTC – Stevenson sends a picture of an individual who appears to be STENSON with another individual who appears to be John Burgdorff[3].
-02/12/2018 – 04:19:26 UTC – Vhasin sends Stevenson a picture of what appears to be two young females, both with dark colored hair, one in a dark colored shirt and the other in a white colored shirt, riding in what appears to be the back of a taxi

h. Chats between the Stevenson account and MSK, who is an identified victim who was interviewed by Philippine authorities in March 2019 and disclosed sexual encounters with STENSON in 2016 when she was under 18 years of age, are as follows:

-04/30/2017 – 05:10:41 UTC – Stevenson: U know where LeCarmen is
-04/30/2017 – 05:10:48 UTC – MSK: yes
-04/30/2017 – 05:11:09 UTC – Stevenson: Can you come now plz.
-04/30/2017 – 05:11:17 UTC – MSK: Okay
-04/30/2017 – 05:11:26 UTC – Stevenson: U can text me if there are any problems.. 09398220050
-04/30/2017 – 05:11:27 UTC – MSK: i log out now!
-04/30/2017 – 05:12:04 UTC – Stevenson: Okay.. Just come to room 304… I will be at the sports center, but my friend is waiting to talk with you.. and share with you..
-05/03/2017 – 06:10:23 UTC – Stevenson: Ok.. be here at 4 for bonding with John and i will give you a hug.
-06/11/2017 – 02:00:14 UTC – MSK: Don? My Birthday is on August 29. Dont forget my Birthday gift hehehehe
-06/11/2017 – 02:01:12 UTC – Stevenson: Ahahaha.. I will try
-06/11/2017 – 02:02:34 UTC – MSK: That's my 18th birthday
-07/22/2017 – 07:20:28 UTC – Stevenson: <3 <3 Thanks for the video chat!

---

[2] Through my training and experience, I have come to understand the word "debut" means 18th birthday.

[3] As noted earlier, John Burgdorff is the individual whose name is registered with Charter Communications as the user of IP addresses used by the Donald White account, and as explained below, is the owner of 2939 S. 101st St., West Allis, WI where STENSON was located and arrested.

16. Between June 25, 2019 and June 27, 2019, forensic interviews were conducted on multiple minor victims who were identified by law enforcement who reside in the Philippines. During the interviews, the females all disclosed having engaged in sexual encounters with STENSON, to include sexual intercourse, while they were under 18 years of age. Each of them also explained that STENSON would pay them in Philippine pesos after the sex acts were completed, and would also give them gifts to include food, clothing, cellphones, computers, and payment for schooling. During the interviews, several of the minors described STENSON as having a grey and black laptop computer (brand unknown), a black HP laptop computer, an Apple iPhone, a Samsung cellphone, and a Samsung tablet. Minor 3 and Minor 4 both stated that STENSON sent their mother, D.C., money via Western Union. After learning this information, records were requested via subpoena from Western Union on June 28, 2019. On July 1, 2019, I received a response from Western Union showing that STENSON sent D.C. $123 U.S. dollars (USD) on June 2, 2017, $78.48 USD on October 29, 2017, and $68.60 USD on January 9, 2018.

17. After having reviewed all of the evidence to include the facts contained in this affidavit, there was probable cause to believe STENSON had engaged in illicit sexual conduct with minors and as such on July 12, 2019, I arrested STENSON with assistance from the City of West Allis Police Department, at the residence of 2939 S. 101st St., West Allis, WI which is owned by John Burgdorff. I knocked on the door and after several minutes of knocking and ringing the doorbell, an individual, later identified as STENSON, exited the residence from the back door of the house. STENSON was placed in handcuffs by West Allis officers for officer safety. Another male, later identified as John Burgdorff, was at the backdoor of the residence and sat on the steps leading to the door. I introduced myself to STENSON and advised STENSON there was a warrant for his arrest for the illicit sexual conduct with minors. STENSON stated to me that he

had written a letter for a judge or a "reader" stating his case, and that such letter was on his computer and that he had not printed it out yet. STENSON stated he needed an attorney as he has been advised that "people are looking for a conviction rather than justice" and "I am innocent" and that he will not be speaking with anyone. STENSON then asked Mr. Burgdorff to print off the letter from his computer, as well as get other documents from his luggage, which were inside the house. Mr. Burgdorff went into the house to obtain the documents requested by STENSON while accompanied by West Allis officers. A short time later, the officers exited the residence with STENSON's Lenovo laptop computer, Samsung cellphone, one piece of luggage and a backpack belonging to STENSON that Mr. Burgdorff provided to the officers. The luggage piece had a baggage tag on it with STENSON'S name and the name and address for Hotel Le Carmen. The officers stated that Mr. Burgdorff stated he wanted all of STENSON's belongings out of his house and that he (Burgdorff) wanted to move on from this. The article of luggage was locked, as it had a built-in lock, consisting of three numeric dials, on it. Two West Allis officers began discussing how the luggage could be opened so the contents could be examined for hazardous material or contraband, and inventoried, as it, and the rest of STENSON's property would be held at the West Allis Police Department over the weekend. STENSON, overhearing the conversation, and without being asked, voluntarily gave the code to his luggage, so it could be examined to ensure there were no dangerous or hazardous items within it. A West Allis officer opened and briefly searched the luggage and backpack in the presence of STENSON. STENSON was asked if he takes any medication, which he said he did. Two medicine bottles were found and placed in the pocket inside the luggage.

18. At approximately 6:55 PM, STENSON was transported to the West Allis Police Department. There, STENSON was inprocessed, fingerprinted and photographed. STENSON's

items were inventoried by the West Allis Police Department and stored as property. During the inventory of STENSON's luggage and backpack, a SanDisk Ultra 32GB micro SD card, a DT101 G2 8GB thumb drive, and a Apacer thumb drive, were found in the backpack. None of the electronic devices were opened, looked through, or any in any way examined, and to date the contents are unknown.

19. On July 15, 2019, HSI Russell Dykema and I picked up STENSON at West Allis Police Department. At the time, STENSON's property was turned over to me and thus the property is currently in HSI Milwaukee's possession. STENSON was transported to the U.S. Marshal's Office at the federal courthouse in Milwaukee, WI where he later had his arraignment before U.S Magistrate.

TECHNICAL TERMS

20. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device. Several minor victims have stated that they observed STENSON with multiple cellphones, to include a Samsung cellphone, which was turned over to authorities during STENSON's arrest.

b. Electronic storage devices: Electronic storage devices includes computers, cellular telephones, tablets, and devices designed specifically to store electronic information (e.g., external hard drives and USB "thumb drives"). Many of these devices also permit users to communicate electronic information through the internet or through the cellular telephone network (e.g., computers, cellular telephones, and tablet devices such as an iPad).

c. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

d. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

21. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

22. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the listed Devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). I know from my training and experience that users can access social media sites like, Facebook and video chatting applications/softwares with both mobile phones and computers and which such access and evidence can remain on the devices. Further, I know from my training and experience that evidence can remain on storage mediums of wire transfers like those from Western Union. I also know that individuals typically store files on their devices that they upload to social media websites and it is easy to transfer saved image, video or other files from one device to another such as saving a file on a computer and transferring it to an external hard drive or SD card.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

23. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the devices consistent with the warrant. The examination may require authorities to employ techniques, including but not

limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

24. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

25. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Devices described in Attachment A to seek the items described in Attachment B.

ATTACHMENT A

The property (here after known as "Devices") to be searched are:

a. Lenovo laptop computer, Serial Number: YB10215587 – located inside residence

b. Black Samsung Cellphone, Serial Number: RF1F6151AVM – located inside residence

c. SanDisk Ultra 32GB Micro SD card, Serial Number: 4226CM32M19y - located in luggage

d. DT101 G2 8GB thumb drive – located in luggage

e. Apacer thumb drive – located in luggage

The Devices are currently at the U.S. Department of Homeland Security Office located at 790 N. Milwaukee Street, Milwaukee, Wisconsin, in evidence.

This warrant authorizes the forensic examination of the Devices for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

1. All records on the Devices described in Attachment A that relate to violations of 18 USC §§ 2423(c) and 1591, including:

   a. Records or information, photographs, videos, notes, documents, or correspondence, in any format or medium, concerning communications about sexual activity with or sexual interest in minors; and

   b. Records or information, notes, documents, or correspondence, in any format or medium, concerning communications about transferring money.

2. All names, aliases, and numbers stored on the Devices, including numbers associated with the Devices, relating to the identities of those engaged in the sexual activity with or sexual interest in minors.

3. Images, videos or visual depictions of minors to include sexually explicit images, videos or visual depictions.

4. Records and information containing sexual activity or sexual interest in minors, including but not limited to texts, images and visual depictions of/or regarding minors.

5. Any and all information, notes, software, documents, records, or correspondence, in any format and medium, pertaining to the listed violations.

6. Any and all address books, names, and lists of names and addresses of individuals who may have been contacted by use of the computer or by other means for the purpose of committing the violations to include any reocrds or information regarding video chatting or like communication software/applications.

7. The list of all telephone calls made or received located in the memory of the Device that provides information regarding the identities of and the methods and means of operation and communication by those engaged in sexual activity with or sexual interest in minors.

8. Any and all information, notes, documents, records, or correspondence, in any format or medium, concerning membership in online groups, clubs, or services that provide or make accessible sexual activity with or sexual interest in minors.

9. Any and all information, records, documents, invoices and materials, in any format or medium, that concern e-mail accounts, online storage, or other remote computer storage pertaining to the violations.

10. Evidence of user attribution showing who used or owned the Device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.